Claims

1. Apparatus for use by a first party for key management for secure communication with a second party, said key management being to provide at each party, simultaneously remotely, identical keys for said secure communication without transferring said keys over any communication link, the apparatus comprising:

a datastream extractor, for obtaining from data exchanged between said parties a bitstream,

a random selector for selecting, from said bitstream, a series of bits in accordance with a randomization seeded by said data exchanged between said parties,

a key generator for generating a key for encryption/decryption based on said series of bits,

thereby to manage key generation in a manner repeatable at said parties.

2. Apparatus according to claim 1, the random selector being operable to use results of said randomization as addresses to point to bits in said datastream.

3. Apparatus according to claim 1, said key generator operable to generate a new key after a predetermined number of message bits have been exchanged between said parties.

4. Apparatus according to claim 3, said predetermined number of message bits being substantially equal to a length in bits of said key.

5. Apparatus according to claim 1, further comprising a control messager for sending control messages to said remote party, thereby to indicate to said remote party a state of said apparatus to enable said remote party to determine whether said remote party is synchronized therewith to generate an identical key.

6. Apparatus according to claim 5, further comprising a synchronized state determiner, for determining from control messages received from a remote party whether said apparatus is synchronized therewith to generate an identical key.

7. Apparatus according to claim 6, further comprising a resynchronizer, associated with said synchronous state determiner, said resynchronizer having a resynchronization random selector for selecting, from a part of said bitstream previously used by said random selector, a series of bits in accordance with a randomization seeded by said data exchanged between said parties,, in the event of determination of synchronization loss, thereby to regain synchronization.

8. Apparatus according to claim 7, wherein said series of bits is a series of bits previously used by said random selector.

9. Apparatus according to claim 6, wherein said control messager is operatively connected to said synchronous state determiner, thereby to include within said control messages a determination of synchronization loss.

10. Apparatus according to claim 7, wherein said control messager is operatively connected with said resynchronizer, to control said resynchronizer to carry out said selection in the event of receipt of a message from said remote party that said remote party has lost synchronization.

11. Apparatus according to claim 7, said data communication being arranged in cycles, said part of said bitstream being exchangeable in each cycle.

12. Apparatus according to claim 11, said cycle being arranged into sub-units, each said cycle having an exchange point at its beginning for carrying out said exchange.

13. Apparatus according to claim 10, said messager being usable to exchange control messages with said remote party to ensure that a same bitstream part is used for resynchronization at both said parties.

14. Apparatus according to claim 12, said messager being usable to vary a control message in accordance with a sub-cycle current at a synchronization loss event, thereby to control said remote party to resynchronize using a same bitstream part.

15. Apparatus according to claim 14, operable to respond to messages sent by a remote party following said synchronization loss event, to revert to same said bitstream part as said message indicates that said remote party intends to use.

16. Apparatus according to claim 1, comprising circuitry for determining which of itself and said remote party is a transmitting party and being operable to control said synchronization when it is a transmitting party and to respond to control commands of said remote party when said remote party is said transmitting party.

17. Apparatus according to claim 6, wherein said synchronized state determiner comprises:

a calculation circuit for carrying out an irreversible calculation on any one of said bitstream, said randomization, said key and derivations thereof, and

a comparator for comparing a result of said calculation with a result received from said remote party,

thereby to determine whether said parties are in synchronization.

18. Apparatus according to claim 17, wherein said irreversible calculation comprises a one-way function.

19. Apparatus according to claim 1, said system being operable to provide key management for a symmetric cryptography algorithm.

20. Apparatus according to claim 19, being constructed modularwise such that said cryptography algorithm is exchangeable.

21. A system for providing key management between at least two separate parties, the system comprising

a primary bitstream for exchange between said parties,

and at each party:

a selector for randomly selecting, at predetermined selection intervals, parts of said primary bitstream to form a derived bit source, each selector being operable to use said derived bit source, in an identical manner, to randomize said selecting, and

a key generator for generating cryptography keys at predetermined key generating intervals using said derived bit source of a corresponding selection interval.

22. A system according to claim 21, wherein said primary bitstream is obtainable as a stream of bits from a data communication process between said two parties.

23. A system according to claim 21, wherein said bits in said primary bitstream are separately identifiable by an address, and wherein said selector is operable to select said bits by random selection of addresses.

24. A system according to claim 21, wherein each selector comprises an address generator and each address generator is identically set.

25. A system according to claim 21, further comprising a controller for exchanging control data between said parties to enable each party to determine that each selector is operating synchronously at each party.

26. A system according to claim 25, wherein said control data includes any one of a group comprising:

redundancy check data, and

a hash encoding result,

of at least some of the bits from said derived bit source.

27. A system according to claim 25, wherein said control data includes any one of a group comprising:

redundancy check data, and

a hash encoding result,

of at least some of the bits of said randomization.

28. A system according to claim 25, wherein said control data includes any one of a group comprising:

redundancy check data, and

a hash encoding result,

of at least some of the bits from said key.

29. A system according to claim 25, wherein said control data includes any one of a group comprising:

redundancy check data of at least some of said addresses, and

a hash encoding result of at least some of said addresses.

30. A system according to claim 25, further comprising at each party a resynchronizer operable to determine from said control data that synchronization has been lost between the parties and to regain synchronization based on a predetermined earlier part of said derived bit source.

31. A system according to claim 22, further comprising at each party a resynchronizer operable to determine from control data exchanged between said parties that synchronization has been lost between said parties and to regain synchronization based on a predetermined earlier part of said derived bit source.

32. A system according to claim 31, said data communication process being arranged in cycles, said predetermined earlier part being exchangeable in each cycle.

33. A system according to claim 32, said cycles being arranged into sub-units, each said cycle having an exchange point at its beginning for carrying out said exchange of said predetermined earlier part of said derived bit source.

34. A system according to claim 30, said controller being usable to include in said control messages, data to ensure that a predetermined earlier part of said derived bit source of a same cycle is used for resynchronization at both said parties.

35. A system according to claim 33, said controller being usable to vary a control message in accordance with a sub-cycle current at a synchronization loss event, thereby to control said remote party to resynchronize using same said predetermined earlier part of said derived bit source.

36. A system according to claim 35, operable to respond to messages sent by a remote party following said synchronization loss event, to revert to same said predetermined earlier part of said derived bit source as said message indicates that said remote party intends to use.

37. A method of key management with at least one remote party, comprising the steps of:

sharing with said remote party a primary data stream,

using said primary data stream to form a randomizer,

selecting parts of said primary data stream using said randomizer to form a derived data source, and

using said derived data source to form cryptography keys at predetermined intervals.

38. A method according to claim 37, wherein said primary data source is obtainable as a stream of bits from a communication process between said two parties.

39. A method according to claim 37, wherein said primary data source comprises a stream of data bits divisible into data units and comprising selecting at random from the data bits of each data unit.

40. A method according to claim 39, wherein said bits in said data units are separately identifiable by addresses, and comprising selecting said bits by using said randomizer as an address pointer.

41. A method according to claim 37, wherein selecting is carried out by using identically set pseudorandom data generation at each party, and using said derived data source as a seed for said pseudorandom data generation.

42. A method according to claim 37, further comprising exchanging control data between said parties to enable each party to determine whether they are operating synchronously with said other party.

43. A method according to claim 42, wherein said control data includes any one of a group comprising:

redundancy check data of at least some of said derived data source, and

a hash encoding result of at least some of said derived data source.

44. A method according to claim 42, comprising determining from said control data that synchronization has been lost between the parties and regaining synchronization based on a predetermined earlier part of said derived data source.

45. A method according to claim 44, further comprising a step of exchanging said predetermined earlier part of said derived data source at predetermined intervals.

46. A method according to claim 45, further comprising steps of:

determining a possibility of each party being at a different cycle at synchronization loss, and

controlling said resynchronization to use a same predetermined earlier part of said derived data source at both parties.

47. A method according to claim 45, further comprising creating in advance a future cycle's predetermined earlier part of said derived data source for resynchronizing with a party that has already moved to such a cycle.

48. A method according to claim 37, in use to provide key management for a symmetric cryptography algorithm.